

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with the Apple IDs and Apple iCloud accounts
associated with mrvazquez@gmail.com (Target Apple iCloud Account),
that is stored at premises owned, maintained, controlled, or operated
by Apple Inc., as further described in Attachment A.

)
)
)
)
)
)
)

Case

No.22-1806M(NJ)

Matter No. 2021R00403

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure
of the following person or property located in the _____ District of _____

(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 11/22/2022 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to _____

Honorable Nancy Joseph

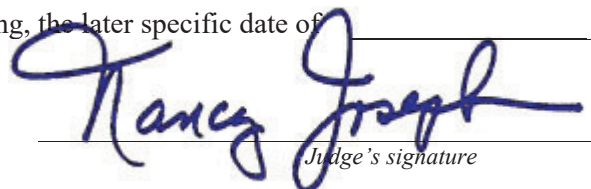
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 11/8/2022 @ 3:01 p.m.

City and state: Milwaukee, Wisconsin



Judge's signature

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

Property to Be Searched

Matter Number 2021R403

This warrant applies to information associated with the Apple IDs and Apple iCloud accounts associated with the following information (**Target Apple iCloud Account**), that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., One Apple Park Way, Cupertino, California 95014.

Apple ID	First Name	Last Name	Date Created	Telephone No.	DSID
mrvazquez@gmail.com	Jv towing	Llc	01/13/2019	414-539-9272	16387276110

ATTACHMENT B
Particular Things to be Seized
Matter Number 2021R403

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the accounts (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber

Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. Contents of all emails associated with the **Target Apple iCloud Account** from **September 1, 2021 to present**, including stored or preserved copies of emails sent to and from the accounts (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the **Target Apple iCloud Account** from **September 1, 2021 to present**, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the accounts (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud

Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the accounts (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the accounts or devices associated with the accounts were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the accounts, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files.

The Provider is hereby ordered to disclose the above information to the government within fourteen days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and/or instrumentalities of distribution and possession with intent to distribute controlled substances, conspiracy to distribute and possess with the intent to distribute controlled substances and maintaining a drug-involved premises, violations of Title 21, United States Code, Sections 841, 846 and 856, have been committed by Alex WEDDLE, Carlos PEREZ- RAMIREZ, Janicia MACK-HOWARD, Marisela OBREGON, Xzayvier WEDDLE, Gerald JONES, Lemar HOWZE, Ramone LOCKE Sr. and other identified and unidentified subjects January 1, 2021 to present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. any information relating to Alex WEDDLE, Xzayvier WEDDLE, Carlos PEREZ-RAMIREZ, Marisela OBREGON, Janicia MACK-HOWARD, Lemar HOWZE, Ramone LOCKE Sr., Joey VAZQUEZ possession or purchase of controlled substances;
- b. lists of customers and related identifying information;
- c. information related to types, amounts, and prices of firearm and drugs trafficked as well as dates, places, and amounts of specific transactions;
- d. any information related to sources of firearms and drugs (including names, addresses, phone numbers, or any other identifying information);
- e. communications related to drug and firearm trafficking, including electronic communications such as text and instant message;
- f. any information recording Alex WEDDLE, Xzayvier WEDDLE, Carlos PEREZ-RAMIREZ, Marisela OBREGON, Janicia MACK-HOWARD, Lemar HOWZE, Ramone LOCKE Sr., Joey VAZQUEZ schedule or travel;
- g. all bank records, checks, credit card bills, account information, and other financial records;
- h. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- i. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- j. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- k. Evidence indicating the subscriber's state of mind as it relates to the crime under

- investigation; and
1. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, ATF may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*Information associated with the Apple IDs and Apple iCloud accounts
associated with mrvazquez@gmail.com (Target Apple iCloud Account),
that is stored at premises owned, maintained, controlled, or operated by
Apple Inc., as further described in Attachment A.

Case No.22-1806M(NJ)

Matter No. 2021R00403

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under
penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the
property to be searched and give its location)*:

See Attachment A.

located in the _____ District of _____, there is now concealed *(identify the
person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
21 U.S.C. §§ 841, 846, & 856	Distribution and possession with intent to distribute controlled substances, conspiracy to distribute and possess with the intent to distribute controlled substances and maintaining a drug-involved premises.

The application is based on these facts:

See Attached Affidavit.

☒ Continued on the attached sheet.☐ Delayed notice of _____ days *(give exact ending date if more than 30 days: _____)* is requested under
18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

ALEXANDER ERLIEN

Digitally signed by ALEXANDER ERLIEN
Date: 2022.11.07 16:58:04 -06'00'*Applicant's signature*

ATF SA Alexander Erlien

*Printed name and title*Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ *(specify reliable electronic means)*

Date: 11/8/2022

City and state: Milwaukee, Wisconsin

Honorable Nancy Joseph, U.S. Magistrate Judge

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT
MATTER NUMBER 2021R403**

I, Alexander Erlien, a Special Agent (SA) with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter “Apple”) to disclose to the government records and other information, including the contents of communications, associated with the **Target Apple iCloud Account** associated with the following information, and further described in Attachment A, that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA:

Apple ID	First Name	Last Name	Date Created	Telephone No.	DSID
mrvazquez@gmail.com	Jv towing	Llc	01/13/2019	414-539-9272	16387276110

2. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

3. I have been a SA with the ATF since September 26, 2018. I was previously employed as Police Officer for the City of Janesville, Wisconsin for approximately five and a half years, and prior to that, I was an Officer in the United States Navy for approximately five years. I have a bachelor’s degree in philosophy from the University of Wisconsin – Madison. I have been involved in numerous investigations involving violations of firearms laws, drug trafficking, human trafficking, and drug possession, resulting in the arrest of numerous criminal defendants and the seizure of illegal firearms and illicit controlled substances.

4. I have received training in the investigation of unlawful possession of firearms and possession of firearms by prohibited persons, as well as drug trafficking and related offenses. I have been trained regarding these offenses and has arrested individuals for federal firearms related offenses, as well as drug trafficking offenses. I have also investigated drug trafficking offenses at the state and federal level, including violations of Title 21, United States Code, Sections 841, 846, and 856. I know from training and experience that those that commit crimes commonly communicate, photograph, videotape, and organize using electronic devices, including by phone call, text message, electronic mail, messaging application, and social media.

5. I have participated in numerous investigations involving the seizure of computers, cellular phones, cameras, and other digital storage devices, and the subsequent analysis of electronic data stored within these devices. I have also participated in investigations involving the use of historical and prospective location information to identify targets, map patterns of travel, corroborate other evidence, and apprehend persons to be arrested. On numerous occasions, this electronic evidence has provided proof of the crimes being investigated and corroborated information already known or suspected by law enforcement. During the course of my investigations, I have regularly used electronic evidence relating to the commission of criminal offenses, including intent, motive, manner, means, and the identity of co-conspirators.

6. I have participated in the execution of numerous search warrants in which weapons, narcotics, and/or evidence of drug trafficking were seized in violation of state and federal laws. I am familiar with the different types and calibers of firearms and ammunition commonly possessed for illegal purposes, as well as the methods used to conduct narcotics trafficking. I have had a variety of formal, informal, and on the job training in the investigation of illegal firearms possession firearms trafficking, and drug trafficking. Additionally, I am familiar with street name(s) of firearms, controlled substances, and respective related topics, as well as has knowledge of the use of money laundering to conceal ill-gotten money.

7. SA Dalton Evertz with the ATF performed various investigative tasks in this matter, including several undercover operations. SA Evertz is employed as a special agent with the ATF and has been since October 2018. SA Evertz received extensive training at the Federal Law Enforcement Training Center in Glynco, GA. SA Evertz attended the Criminal Investigator Training Program, as well as ATF's Special Agent Training Program. SA Evertz has received training in the investigation of violations of firearms laws, drug trafficking, and drug possession. SA Evertz has gained experience in the conduct of such investigations through previous case investigations, formal training, and in consultation with law enforcement partners in local, state, and federal law enforcement agencies. Prior to becoming a special agent with the ATF, SA Evertz received a bachelor's degrees from the University of Wisconsin – Eau Claire in the field of Criminal Justice. I have discussed and participated this investigation with SA Evertz.

8. Information contained in this affidavit was either obtained directly by me or by other investigators who I believe to be truthful and credible. The facts in this affidavit come from personal observations, training and experience, and information obtained from other investigators and witnesses.

9. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

10. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that possible crimes of distribution and possession with intent to distribute controlled substances, conspiracy to distribute and possess with the intent to distribute controlled substances and maintaining a drug-involved premises, violations of Title 21, United States Code, Sections 841, 846 and 856 have been committed by Alex WEDDLE, Xzayvier WEDDLE, Carlos PEREZ-RAMIREZ, Marisela OBREGON, Janicia MACK-HOWARD, Lemar HOWZE, Ramone LOCKE Sr., Joey VAZQUEZ and other known and unidentified subjects. There is also probable cause to search the information described in Attachment A for evidence of

these crimes further described in Attachment B.

II. JURISDICTION

11. The court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

III. PROBABLE CAUSE

12. In August of 2021, ATF SAs, and Task Force Officers (TFOs) (hereinafter “Case Agents” and/or “Investigators”) began investigating an armed drug trafficking organization (ADTO) operating in the Eastern District of Wisconsin (WI). Over the next eight months, case agents utilized an undercover ATF agent (UCA) to conduct multiple controlled purchases of cocaine/crack cocaine and dry meetings with ADTO members. During some of these meetings the members of the ADTO were armed with firearms. Investigators identified the following individuals as ADTO members: Ramone LOCKE; Alex WEDDLE; Carlos PEREZ-RAMIREZ; Lemar HOWZE; Xzayvier WEDDLE; Gerald JONES; Janicia MACK-HOWARD; and Marisela OBREGON. Many of these individuals have recently been charged with related offenses. *See United States v. Locke, et al.*, 22-CR-133, Dkt. 21 (E.D. Wis. July 19, 2022).

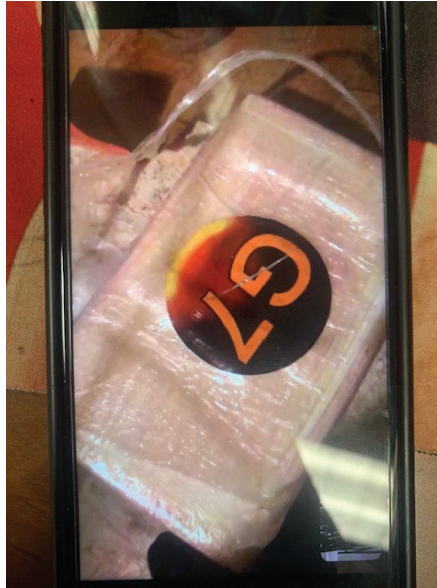
13. Between September 1, 2021, and April 28, 2022, the UCA conducted twelve undercover controlled buys from various member of the ADTO. UCA obtained a total of 140.81 grams (more than five ounces) of crack cocaine and 1316.12 grams (1.316 kilograms) of cocaine from the ADTO in this way. Through the undercover controlled buys and investigation into the ADTO, case agents identified the ADTO used telephone numbers 414-722-0553, 414-517-5178, and 414-627-7500 to conduct their illegal activities. Case agents also identified telephone number 414-748-7363 as WEDDLE’s personal number. All the undercover buys were recorded, and the controlled substances field-tested positive for cocaine. Also, during the undercover controlled buys, the UCA

often observed members of the ADTO with additional amounts of suspected controlled substances package to be sold to drug customers.

14. On February 22, 2022, UCA had an undercover meeting with Alex WEDDLE to discuss future drug sales. Alex WEDDLE disclosed that he communicated with his cocaine source via FaceTime, which is an encrypted video-calling application exclusive to Apple devices (iPhones). Case agents know through training and experience that iPhone users have the option to link an Apple ID/iCloud account to their Apple Devices (i.e., iPhone). iCloud is the service from Apple that stores an account user's photos, files, notes, passwords, messages, and other data in Apple's cloud, and keeps the data/records up to date in all of the user's devices.

15. Beginning in February of 2022, Investigators identified that the ADTO's cocaine source was Ramone LOCKE Sr. based on statements provided by Alex WEDDLE, FaceTime logs analysis, jail calls, and database searches. Ramone LOCKE Sr. employed an Apple iPhone utilizing telephone number 414-578-7810. Further investigative techniques revealed the iCloud account tied to this iPhone was "ramone.locke@icloud.com".

16. On April 22, 2022, Alex WEDDLE, using number 414-748-7363, called UCA via FaceTime. During this FaceTime call, Alex WEDDLE showed UCA a suspected kilogram of cocaine in Alex WEDDLE's possession (Figure 1). This suspected kilogram of cocaine related to the prior meeting between Alex WEDDLE and UCA had regarding pooling their money together to purchase a kilogram of cocaine from Alex WEDDLE's source.



(Figure 1)

Screenshot of suspected kilogram of cocaine shown to UCA by Alex WEDDLE via FaceTime

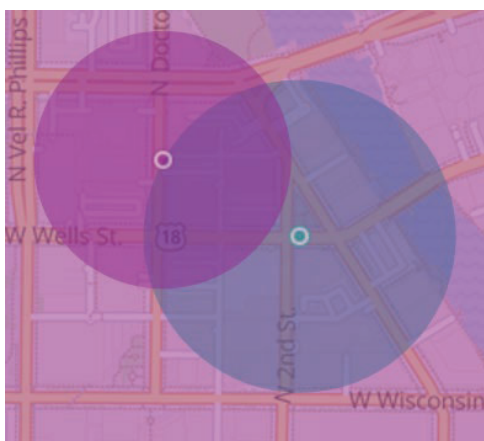
17. On May 10, 2022, the Honorable Nancy Joseph authorized the search of the records and information (including contents of communications) associated with ramone.locke@icloud.com for the time period of January 1, 2021, to May 10, 2022. On May 16, 2022, Apple, Inc. provided Investigators with the aforementioned records and information. Case Agents are currently working to review the contents of the account.

18. Case agents reviewed the FaceTime, call detail records, and mobile location data obtained through federal search warrants and subpoenas for the date April 22, 2022, when Alex WEDDLE FaceTime UCA with the kilogram of cocaine. The only contacts Alex WEDDLE had using number 414-748-7363 on April 22, 2022, day was with ADTO telephone numbers, another number associated with Alex WEDDLE, the UCA's number, and Ramone LOCKE Sr.'s number (414-578-7810). In fact, approximately four minutes prior to Alex WEDDLE calling UCA, Alex WEDDLE FaceTime called Ramone LOCKE Sr.

19. Further examination of the FaceTime call detail records for the ADTO's drug customer line 414-517-5178 from April 22, 2022, revealed that from approximately 3:45 P.M. until 5:56 P.M., 414-517-5178 communicated with LOCKE Sr.'s number 414-578-7810 via FaceTime

a total of seven times. Case agents reviewed the mobile device location data for Alex WEDDLE's number 414-748-7363. At approximately 3:45 P.M., which is the time 414-517-5178 first called LOCKE Sr.'s number 414-578-7810 via FaceTime, Alex WEDDLE's mobile device, 414-748-7363, was in the vicinity of 3266 North 35th Street, Milwaukee, WI, which case agents determined was a residence used by WEDDLE and other ADTO members. Agents observed that the cellular device associated with Alex WEDDLE's telephone number 414-748-7363 remained within the vicinity of 3266 North 35th Street until approximately 5:54 P.M., which is when Alex WEDDLE's the cellular device 414-748-7363 was identified to be in downtown Milwaukee. Please note, the distance from 3266 North 35th Street to downtown Milwaukee is approximately five miles. Agents also observed that at approximately 5:54 P.M., the cellular device associated with LOCKE Sr.'s phone 414-578-7810 was in close proximity to Alex WEDDLE's cellular device of 414-748-7363 in downtown Milwaukee.

20. After the mobile device location data was collected at 5:54 P.M., the next mobile device location data that was collected for LOCKE Sr.'s phone 414-578-7810 and Alex WEDDLE's phone 414-748-7363, occurred at approximately 6:09 P.M. At this time, the mobile device "ping" radii, which were both less than 150 meters, were overlapping (Figure 2). Additionally, agents identified that both LOCKE Sr.'s and Alex WEDDLE's mobile devices had been in different locations at the time of the previous cellular-location data collection (approximately 5:54 P.M.), which agents understood to mean both devices had traveled to this location in downtown Milwaukee for an undetermined amount of time.



(Figure 2)

Cell-Site location data for mobile devices linked to 414-748-7363 (Alex WEDDLE/Purple) and 414-578-7810 (LOCKE Sr./Teal) at approximately 6:09 P.M.

21. Agents then reviewed mobile device location data for the ADTO's drug customer line commonly used by Alex WEDDLE, 414-627-7500, around 6:09 P.M. Agents identified that at approximately 6:05 P.M., the cell-site location data identified the mobile device associated with 414-627-7500 was also within the overlapping cellular-location radii of Alex WEDDLE's phone 414-748-7363 and LOCKE Sr.'s phone 414-578-7810. A visual map of the cell-site location data is contained within Figure 3.



(Figure 3)

Map showing cellular-location data overlaps of 414-627-7500 (yellow) at approximately 6:05 P.M., and 414-748-7363 (purple)/414-578-7810 (teal) at approximately 6:09 P.M.

22. Case agents also collected two other mobile device location data points for LOCKE Sr.'s phone 414-578-7810 and Alex WEDDLE's 414-748-7363 after this 6:09 P.M.

point but before Alex WEDDLE used 414-748-7363 to call UCA via FaceTime and displayed a suspected kilogram of cocaine (approximately 6:49 P.M.).

23. The first mobile device location data point, collected at approximately 6:24 P.M., identified the Alex WEDDLE's mobile device 414-748-7363 had traveled back towards 3266 N 35th Street while LOCKE Sr.'s mobile device 414-578-7810 had moved to a different location in downtown Milwaukee. The second mobile device location data point, collected at approximately 6:39 P.M., identified Alex WEDDLE's mobile device 414-748-7363 had returned within the vicinity of 3266 N 35th Street, while the mobile device associated with LOCKE Sr.'s mobile device 414-578-7810 had remained near downtown Milwaukee.

24. On April 22, 2022, at approximately 6:49 P.M., Alex WEDDLE used 414-748-7363 to call UCA via FaceTime and showed UCA a suspected kilogram of cocaine in Alex WEDDLE's possession. This call occurred approximately 40 minutes after the cellular devices associated with Alex WEDDLE number 414-748-7363 and LOCKE Sr. number 414-578-7810 were within overlapping cell-sectors.

25. On June 7, 2022, law enforcement located LOCKE Sr. in the Northern District of Illinois, where they observed him, inter alia, placing a black bag into his Audi A5. The Audi had a suspected illegal window tint and only bore a rear Wisconsin license plate. Racine County Sheriff Deputies stopped the Audi traveling northbound I-94 in Racine County, Wisconsin. The driver and sole occupant was LOCKE Sr. Deputy Allard, who is a certified narcotics canine (K-9) handler, and his K-9 Zeke were present during the traffic stop. Together, Deputy Allard and Zeke are a certified Police Narcotic Detection Team.

26. Deputy Allard and Zeke passed around the outside of LOCKE Sr.'s Audi while another Racine County Sheriff's Deputy continued to conduct the traffic stop. Deputy Allard watched as Zeke alerted to LOCKE Sr.'s Audi, consistent with Zeke detecting the odor of controlled substances. Based on Zeke's alert, Deputies conducted a search of LOCKE Sr.'s Audi.

27. Deputies searched the dashboard area to the left of the steering wheel in LOCKE Sr.'s Audi. Deputies then observed a hidden compartment in that same area. Based on training and experience, Investigators are aware drug traffickers commonly use hidden compartments installed in vehicles to conceal controlled substances to evade law enforcement detection. These hidden compartments are commonly referred to as a "trap."

28. Deputies were not able to fully access the hidden compartment but were able to observe a clear plastic bag and a black plastic bag inside – the latter of which was consistent in appearance with the bag Investigators saw LOCKE Sr. place inside the Audi earlier. Deputies had limited access to this hidden compartment on-scene, but they were able to use a knife to cut into the clear bag which contained a white substance. Deputies used a Sirchie Nark Cocaine I.D. Swipe to test the white powdery substance, which tested positive for the presence of cocaine.

29. LOCKE Sr. initially would not get out of his vehicle when instructed, but he complied after approximately two minutes. LOCKE Sr. also acknowledged that the vehicle was his, though he indicated that he would occasionally let other persons drive it.

30. During the stop, law enforcement located the following two phones:

- a. A black iPhone (unknown serial number) taken from the front passenger seat of the Gray 2018 Audi A5. Later inventoried as Racine County Sheriff's Office Item #22-001217-7; and
- b. A black iPhone (unknown serial number) taken from Ramone J. LOCKE Sr. Later inventoried as Racine County Sheriff's Office Item #22-001217-8.

31. Deputies could not fully access the hidden compartment to remove the suspected controlled substances on-scene. Deputies therefore towed LOCKE Sr.'s Audi to the Racine County Sheriff's Substation and obtained a state search warrant, in order to further gain access to the hidden compartment. Deputies eventually were able to gain access to the hidden compartment and located

approximately two kilograms of a white powdery substance that field-tested positive for cocaine and fentanyl (though later laboratory testing would confirm only the presence of cocaine). Based on my training, experience, and investigation in this ADTO, this large amount of narcotics is consistent with the sale of controlled substances.

32. On June 7, 2022, SA Evertz sent a preservation request to Apple, Inc. for data and records pertaining to the iCloud account associated with 414-578-7810 (ramonelocke@iCloud.com/DSID 17409862088 and 17407597786).

33. On June 10, 2022, Honorable William E. Duffin, U.S. Magistrate Judge, authorized the search of the two iPhones recovered from LOCKE's Audi.

34. On June 13, 2022, SA Evertz and TFO Malafa obtained the aforementioned iPhones from the Racine County Sheriff's Office. SA Evertz and TFO Malafa then transported the devices to the ATF Milwaukee Field Office, where the devices were entered into ATF evidence as Property Item Nos. 21 and 22.

35. On June 15, 2022, SA Evertz transported the two iPhones recovered from LOCKE's Audi to the Great Lakes High Intensity Drug Trafficking Area Office (HIDTA) in Milwaukee, WI. SA Evertz transferred the devices to HIDTA Digital Forensics Analyst (DFA) Brant Ungerer for extraction.

36. On June 16, 2022, DFA Ungerer performed an extraction on the iPhones' Subscriber Identity Module (SIM) card, which identified the telephone numbers associated with the respective devices. Through this SIM card extraction, process, the Mobile Station Integrated Services Digital Networks (MSISDN/Telephone Number) were identified as follows:

- a. 414-578-7810 – Gray/Black iPhone recovered from LOCKE Sr.'s Audi (ATF Item No. 21).
- b. 414-712-5531 – Black iPhone recovered from LOCKE Sr.'s Audi (ATF Item No. 22).

37. It is important to note that DFA Ungerer performed extractions solely on the devices' SIM cards. Therefore, case agents do not possess complete device extraction reports. Law enforcement is continuing to attempt to develop complete extraction reports for both devices.

38. On August 12, 2022, SA Evertz sent a preservation request to Apple, Inc. for data and records pertaining to the iCloud account associated with 414-712-5531. Please note, at the time SA Evertz sent this preservation request, case agents were unaware of any iCloud accounts associated with telephone number 414-712-5531.

39. On August 15, 2022, SA Evertz served Apple, Inc. with a Grand Jury Subpoena, which sought subscriber information and account holder records for iCloud accounts tied to 414-712-5531.

40. On August 20, 2022, Apple, Inc. provided SA Evertz with Account Details for the iCloud account associated with 414-712-5531:

- a. Apple ID: LLB4LIFE3278@icloud.com
- b. DSID: 20262782484
- c. Creation Date: May 26, 2021
- d. First/Last Name: "Amir Lock" and "Ramone LOCKE"
- e. Address: 2707 N 41st Street, Milwaukee, WI 53210
- f. Verified Phone Number: 414-712-5531
- g. Business Phone Number: 414-578-7810

41. Over the course of the investigation, SA Evertz has learned that Amir Locke is Ramone LOCKE Sr.'s elder, deceased brother, and LOCKE Sr.'s address listed on his State of Wisconsin Driver's License is 2707 N 41st Street, Milwaukee, WI. Furthermore, SA Evertz knows through training and experience that narcotics traffickers often falsify their telephone number's subscriber information to avoid detection by law enforcement.

42. On August 23, 2022, SA Evertz identified an obituary for Amir Locke after

querying Amir Locke's name via an open-source internet search. Per reidsgoldengate.com, Amir Locke passed away on November 9, 2020. SA Evertz identified from the records received from Apple, Inc. on August 20, 2022, the name on the billing profile within the "Apple Media Services Data" changed from "Amir Lock" to "Ramone LOCKE," with an effective date of January 29, 2022.

43. It is important to again note that on May 10, 2022, the Honorable Nancy Joseph authorized the search of records and information located within the iCloud account of ramonelocke@icloud.com (Search Warrant No. 22-873M (NJ)). On September 1, 2022, SA Evertz received authorization to review the communications (iMessage, email, etc.) located within the iCloud account. Please note, the communications within the iCloud account had been scrubbed of any/all attorney-client communications by a "filter team" of ATF SAs and AUSAs who were not involved in the investigation of WEDDLE's DTO and WEDDLE's cocaine source, LOCKE.

44. From the iMessages between LOCKE and WEDDLE, SA Evertz identified that WEDDLE had been receiving cocaine from LOCKE as early as September of 2021.

45. On August 12, 2022, SAs Dalton Evertz and Alex Erlie, along with Assistant United States Attorneys (AUSAs) Katherine Halopka-Ivery and Kevin Knight conducted a proffer interview with Alex WEDDLE (who will at from this point on be referred to as "CI #1")¹. The interview took place at the United States Attorney's Office in Milwaukee, WI. CI #1's defense counsel, Michelle Jacobs, was also present for this interview.

46. During this proffer interview, CI #1 was shown a WI Department of Transportation (DOT) Photograph of Joey VAZQUEZ (M/W; DOB: XX/XX/1985), an individual known to law

¹ CI #1's information is credible and reliable because CI #1 has given information concerning individuals involved in illegal activities, including self-incriminating statements, which has been independently verified through this investigation including queries of law enforcement databases, prior electronic and physical surveillance, review of content from electronic sources, undercover controlled transactions, and other witnesses' statements. CI #1 has a felony conviction for burglary and misdemeanor convictions for possession of cocaine, intimidation of a witness, and resisting or obstructing an officer. CI #1 has no arrests or convictions relating to dishonesty. CI #1 is under a proffer from the United States Attorney's Office and no promises have been provided to CI #1.

enforcement as one of Ramone LOCKE's associates. CI #1 initially stated he did not know the individual in the photo, but explained it looked similar to a Puerto Rican male he knew. SA Evertz then showed CI #1 a photograph of VAZQUEZ from VAZQUEZ's public Facebook account. CI #1 stated the individual in both the DOT photograph and the photograph from VAZQUEZ's Facebook was an individual known to CI #1 as "Joe," "Puerto Rican Joey," and "Joe VAZQUEZ." CI #1 also disclosed that VAZQUEZ drove a tow truck and may have a legitimate tow-truck company.

47. CI #1 stated not long after LOCKE was arrested by law enforcement with 1.995 kilograms of cocaine on June 7, 2022, VAZQUEZ met with CI #1 at BP (Gas Station) located at 2426 N Farwell Ave, Milwaukee, WI 53211, which is located on Milwaukee's eastside. CI #1 stated that during this meeting, which was arranged by VAZQUEZ, CI #1 paid VAZQUEZ \$6,000, which had been owed to LOCKE by CI #1. CI #1 affirmed that VAZQUEZ had collected this money on LOCKE's behalf. Please note, SA Evertz knows through knowledge, training, and experience that the heads of drug trafficking organizations commonly have individuals who collect drug debts on behalf of the DTO, which are often referred to as "collectors," "enforcers," and/or "lieutenants."

48. On September 20, 2022, SA Evertz continued reviewing iMessages within LOCKE's iCloud account. With the knowledge that VAZQUEZ had collected a drug debt from WEDDLE on LOCKE's behalf, SA Evertz reviewed LOCKE's iCloud contacts. SA Evertz identified one of LOCKE's iCloud contacts as "JV (Joey VAZQUEZ) Towin," which was assigned telephone number 414-539-9272. SA Evertz further identified that, with respect to LOCKE's iMessages, "JV Towin"/414-539-9272 was the third-most contacted telephone number by LOCKE (414-578-7810). From March 3, 2021, until May 4, 2022, LOCKE had exchanged 8,067 iMessages with 414-539-9272 (VAZQUEZ).

49. SA Evertz then reviewed the contents of the iMessages between LOCKE (414-578-7810) and 414-539-9272 (VAZQUEZ). SA Evertz identified numerous messages that are consistent with LOCKE discussing drug debt collections with VAZQUEZ. In review of these messages SA

Evertz located the terms “key”, “middle man” and “cheese”. SA Evertz knows through training and experience that “key” is common street vernacular used to reference a kilogram of a controlled substance (I.e., cocaine). SA Evertz knows through training and experience that “cheese” is common street vernacular used to reference U.S. Currency. Additionally, SA Evertz knows through training and experience that an individual who coordinates a drug deal between a drug source and a drug customer is referred to, in street vernacular, as a “middle man.” Some of these messages between LOCKE (414-578-7810) and VAZQUEZ (414-539-9272) are reflected as follows:

a. March 28, 2021 –

LOCKE: Wyo (what you on)
VAZQUEZ: Just walking to the baby shower l
VAZQUEZ: You
LOCKE: Aw ok hit me wen u leave
VAZQUEZ: Ok
LOCKE: U still dere
LOCKE: ?
VAZQUEZ: Yea
VAZQUEZ: 10 min
LOCKE: Ok
VAZQUEZ: Who
LOCKE: Mitch n moe
VAZQUEZ: Ok
LOCKE: Tell Mitch I’m waitin on da key wen u c him
VAZQUEZ: Ok

b. September 22, 2021 –

LOCKE to VAZQUEZ: I watch u middle man 500 to 1000 were is da money.

c. January 15, 2022 –

LOCKE to VAZQUEZ: Can u please pick dis money up frm dude.

d. May 13, 2021 -

LOCKE: Aye grab dat frm Rick.
LOCKE: Wen u can
VAZQUEZ: Ok I got you
LOCKE: Tell him it’s gon b a day or 2
VAZQUEZ: Ok
LOCKE: U get up wit Rick?

LOCKE: Moe ready 2
VAZQUEZ: I was watching the baby while she was at an appointment
I'm just coming back outside now about to go ot Rick
VAZQUEZ: I'll call him 02
LOCKE: Ok
...
LOCKE: U took care of both
VAZQUEZ: Yup

e. May 14, 2021 –

LOCKE: I need u 2 meet Danny in da outlet if not 2day early morning
LOCKE: Give him 8500
VAZQUEZ: OK cool whatever you need me to do let me know
LOCKE: U wanna do it 2day or mornin
LOCKE: *unknown image*
VAZQUEZ: I can do it now
LOCKE: Well hit him n get an understanding
VAZQUEZ: Ok
VAZQUEZ: How much did Rick give me yesterday
VAZQUEZ: I was just about to go run through it
LOCKE: U sldve (should have) counted it
LOCKE: He owed 11,5 (\$11,500), but mayb only gave u 11
LOCKE: Moe owed 44

f. January 3, 2022 –

LOCKE: Wya (Where you at)
LOCKE: Aye go by pourmans grab dat frm (from) TD
**SA Evertz knows from experience that Pourmans is a bar in downtown Milwaukee, WI*
LOCKE: N my guy gon pull up rite dere
LOCKE: Dnt (don't) take Nthn (nothing) doe (though)
VAZQUEZ: Ok
VAZQUEZ: Now [?]
LOCKE: He dere now
LOCKE: Yes
VAZQUEZ: Ok
VAZQUEZ: Leave what I got here
LOCKE: Yes
LOCKE: He finna get u 5500 take 2k n my guy finna (going to) pull up
give him da rest
VAZQUEZ: Ok
LOCKE: Wya
VAZQUEZ: I was about to use the bathroom I stop so I can go do this
VAZQUEZ: I'm here
LOCKE: Get in car wit TD grab da cheese n take 2k
LOCKE: *Unknown image/emoji*
LOCKE: U c him?

LOCKE: He said it was 6
LOCKE: Wat is wrng (wrong) bro dis (did) u count da money
VAZQUEZ: Yea

g. April 21, 2022 –

LOCKE: Wya (Where you at)
VAZQUEZ: TJ *crying laughing emoji*
LOCKE: How is it
VAZQUEZ: It was ok
LOCKE: U take dat key 2 ol boy
VAZQUEZ: He's on his way to me now
LOCKE: Tell him exactly wat I said (VAZQUEZ liked this message via iMessage)
VAZQUEZ: I already know (LOCKE liked this message via iMessage)

h. March 11, 2022 –

LOCKE: I need u 2 give sumbdy 1200 fo me
LOCKE: *Unknown image/emoji
LOCKE: Wen can u do it
VAZQUEZ: I'll call him right now and tell him I have to go pick it up
LOCKE: Ok call him now
VAZQUEZ: Ok
VAZQUEZ: Yep I talk to him
LOCKE: Ok
LOCKE: Man wats da problem bro?
LOCKE: U ant have da 1200?
VAZQUEZ: Yeah I'm just waiting to bump heads with him
LOCKE: U cldve (could have) just got it frm (from) da crib
VAZQUEZ: He said he's gonna call me in a couple minutes when he comes out
LOCKE: Man I asked u earlier 2 do dat fo me
VAZQUEZ: I talk to him like five times

i. April 24, 2022 –

LOCKE: I need u
LOCKE: Ima call u wen I leave out
VAZQUEZ: Ok
LOCKE: *unknown image/emoji*
VAZQUEZ: She's five minutes away I'm out her house
LOCKE: Ight
LOCKE: Finna send u his number
LOCKE: *Unknown message content* (suspected contact card)
VAZQUEZ: Ok
VAZQUEZ: You seen him before

LOCKE: Wym (what do you mean)
VAZQUEZ: That was not for you my fault
LOCKE: U took care of dat?
VAZQUEZ: Yea

50. On September 20, 2022, SA Evertz queried VAZQUEZ's number "414-539-9272" within open-source, commercial websites, which provided the telephone number was associated with "Joey M. VAZQUEZ" and "JVTOWINLLC." On the same date, SA Evertz queried "414-539-9272" via ZetX.com, which identified the mobile carrier for that number as T-Mobile (hereinafter "Service Provider").

51. On September 21, 2022, an administrative subpoena was sent to T-Mobile requesting call detail records and subscriber information for VAZQUEZ's number 414-539-9272. On September 22, 2022, SA Evertz received the requested information from T-Mobile. The subscriber information identified the subscriber as "JVTOWINLLC" with a service address of 456 E Brown APT 403, Milwaukee, WI 53212. The call detail records identified that telephone number 414-539-9272 was active and still making/receiving telephone calls as of September 20, 2022. SA Evertz also queried "456 E Brown Street, Apt 403, Milwaukee, WI 53212" within open-source, commercial databases, and identified VAZQUEZ was associated with this address.

52. On September 30, 2022, Honorable William E. Duffin signed search warrant 22-MJ-168, which sought records and information from T-Mobile for the cellular device assigned call number 414-539-9272. On October 3, 2022, case agents received subscriber and billing information for the aforementioned telephone number:

- a. MSISDN Number (Telephone Number): 414-539-9272
- b. Subscriber Name: JVTOWINLLC
- c. Subscriber Address: 456 E BROWN APT 403, MILWAUKEE, WI 53212
USA
- d. Subscriber Status: Active

e. IMSI: 310260274466454

53. On October 13, 2022, SA Evertz sent a grand jury subpoena to Apple, Inc., for subscriber information and account holder records pertaining to the iCloud account associated with telephone number 414-539-9272. On November 2, 2022, SA Evertz received a response from Apple, Inc., which identified there was an active iCloud account linked to telephone number 414-539-9272. Additionally, the records received from Apple, Inc., provided the following account information:

- a. **Apple ID: mrvazquez089@gmail.com (The Target Apple iCloud Account)**
- b. DSID: 16387276110
- c. First Name: Jv towing
- d. Last Name: Llc
- e. Created On: January 13, 2019
- f. Additional Phone Numbers: 414-793-3446 and 414-639-7785

54. I believe **mrvazquez089@gmail.com (The Target Apple iCloud Account)** contains valuable information that could be used as evidence for the possible crimes distribution and possession with intent to distribute controlled substances, conspiracy to distribute and possess with the intent to distribute controlled substances and maintaining a drug-involved premises, violations of Title 21, United States Code, Sections 841, 846 and 856.

III. INFORMATION REGARDING APPLE ID AND ICLOUD²

55. Apple is a United States company that produces the iPhone, iPad, and iPod Touch,

² The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

56. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.
- c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services and can also be used to store iOS device backups and data associated with third-party apps.
- d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.
- e. Game Center, Apple’s social gaming network, allows users of Apple devices to play and share games with each other.
- f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.
- g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.

- h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

57. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

58. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

59. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and

other log files that reflect usage of the account.

60. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

61. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

62. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo

Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

63. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

64. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

65. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date, and

time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

66. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

67. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

68. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

IV. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

69. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including

the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

V. CONCLUSION

70. Based on the forgoing, I request that the Court issue the proposed search warrant.

71. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

Matter Number 2021R403

This warrant applies to information associated with the Apple IDs and Apple iCloud accounts associated with the following information (**Target Apple iCloud Account**), that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., One Apple Park Way, Cupertino, California 95014.

Apple ID	First Name	Last Name	Date Created	Telephone No.	DSID
mrvazquez@gmail.com	Jv towing	Llc	01/13/2019	414-539-9272	16387276110

ATTACHMENT B
Particular Things to be Seized
Matter Number 2021R403

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the accounts (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber

Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. Contents of all emails associated with the **Target Apple iCloud Account** from **September 1, 2021 to present**, including stored or preserved copies of emails sent to and from the accounts (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the **Target Apple iCloud Account** from **September 1, 2021 to present**, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the accounts (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud

Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the accounts (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the accounts or devices associated with the accounts were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the accounts, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files.

The Provider is hereby ordered to disclose the above information to the government within fourteen days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and/or instrumentalities of distribution and possession with intent to distribute controlled substances, conspiracy to distribute and possess with the intent to distribute controlled substances and maintaining a drug-involved premises, violations of Title 21, United States Code, Sections 841, 846 and 856, have been committed by Alex WEDDLE, Carlos PEREZ- RAMIREZ, Janicia MACK-HOWARD, Marisela OBREGON, Xzayvier WEDDLE, Gerald JONES, Lemar HOWZE, Ramone LOCKE Sr. and other identified and unidentified subjects January 1, 2021 to present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. any information relating to Alex WEDDLE, Xzayvier WEDDLE, Carlos PEREZ-RAMIREZ, Marisela OBREGON, Janicia MACK-HOWARD, Lemar HOWZE, Ramone LOCKE Sr., Joey VAZQUEZ possession or purchase of controlled substances;
- b. lists of customers and related identifying information;
- c. information related to types, amounts, and prices of firearm and drugs trafficked as well as dates, places, and amounts of specific transactions;
- d. any information related to sources of firearms and drugs (including names, addresses, phone numbers, or any other identifying information);
- e. communications related to drug and firearm trafficking, including electronic communications such as text and instant message;
- f. any information recording Alex WEDDLE, Xzayvier WEDDLE, Carlos PEREZ-RAMIREZ, Marisela OBREGON, Janicia MACK-HOWARD, Lemar HOWZE, Ramone LOCKE Sr., Joey VAZQUEZ schedule or travel;
- g. all bank records, checks, credit card bills, account information, and other financial records;
- h. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- i. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- j. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- k. Evidence indicating the subscriber's state of mind as it relates to the crime under

- investigation; and
1. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, ATF may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.